FIG. 1

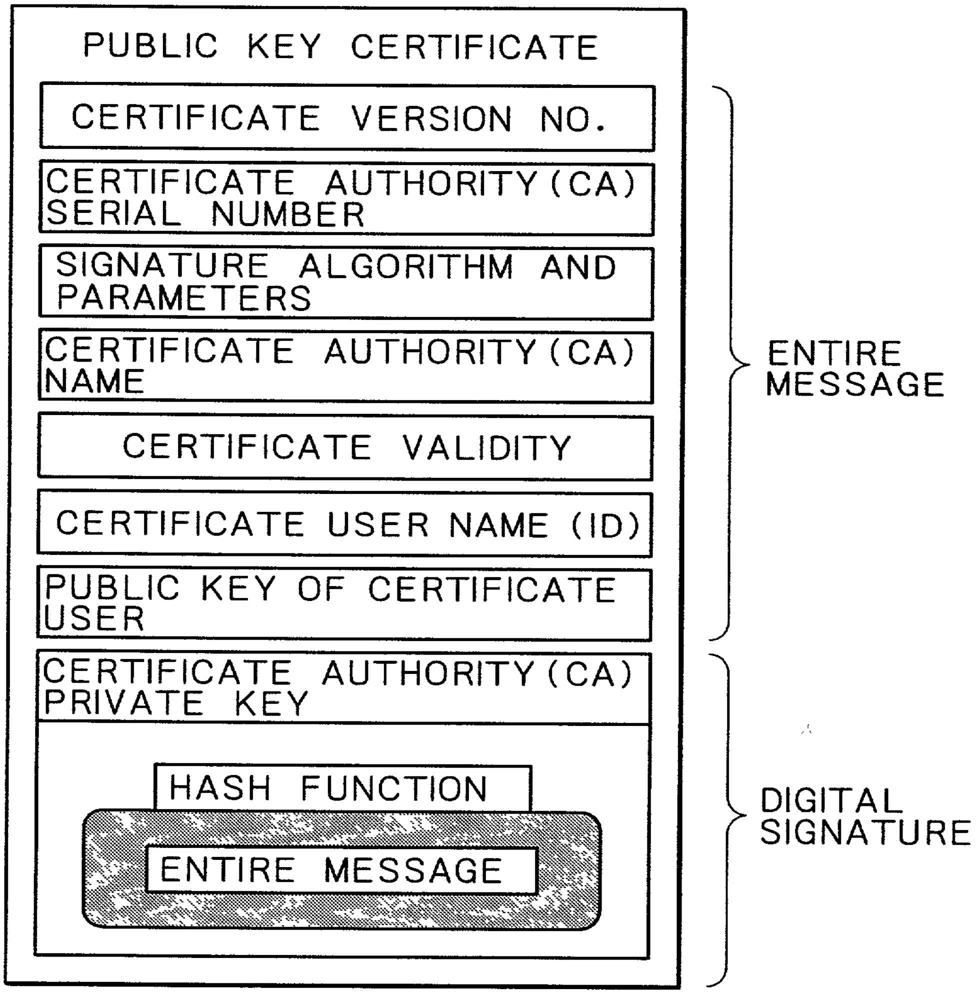

PUBLIC KEY CERTIFICATE
CERTIFICATE VERSION NO.
CERTIFICATE AUTHORITY (CA) SERIAL NUMBER
SIGNATURE ALGORITHM AND PARAMETERS
CERTIFICATE AUTHORITY (CA) NAME
CERTIFICATE VALIDITY
CERTIFICATE USER NAME (ID)
PUBLIC KEY OF CERTIFICATE USER
CERTIFICATE AUTHORITY (CA) PRIVATE KEY
HASH FUNCTION
ENTIRE MESSAGE
ENTIRE MESSAGE
DIGITAL SIGNATURE

FIG.2

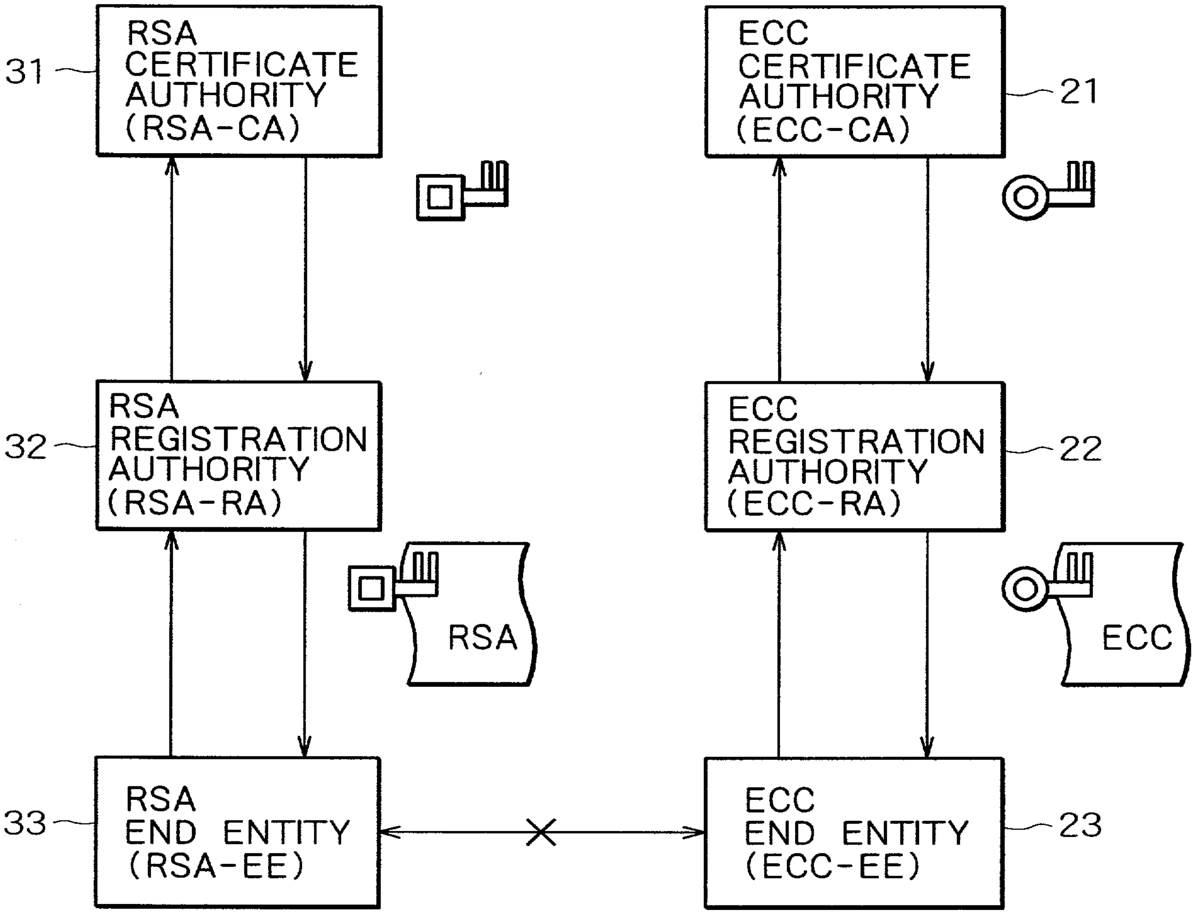

31
RSA CERTIFICATE AUTHORITY (RSA-CA)
ECC CERTIFICATE AUTHORITY (ECC-CA)
21
32
RSA REGISTRATION AUTHORITY (RSA-RA)
ECC REGISTRATION AUTHORITY (ECC-RA)
22
RSA
ECC
33
RSA END ENTITY (RSA-EE)
ECC END ENTITY (ECC-EE)
23

FIG.3

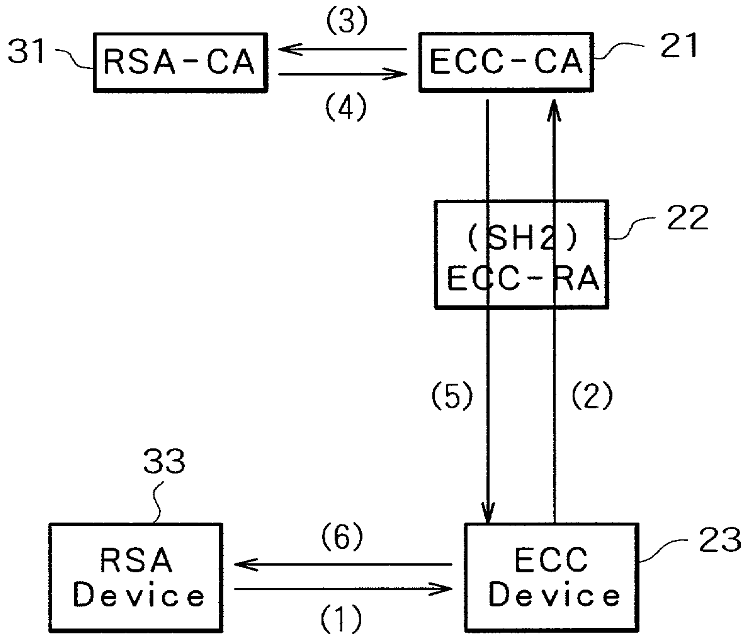

31
RSA-CA
(3)
(4)
ECC-CA
21
(SH2)
ECC-RA
22
(5)
(2)
33
RSA
Device
(6)
(1)
ECC
Device
23

FIG.4

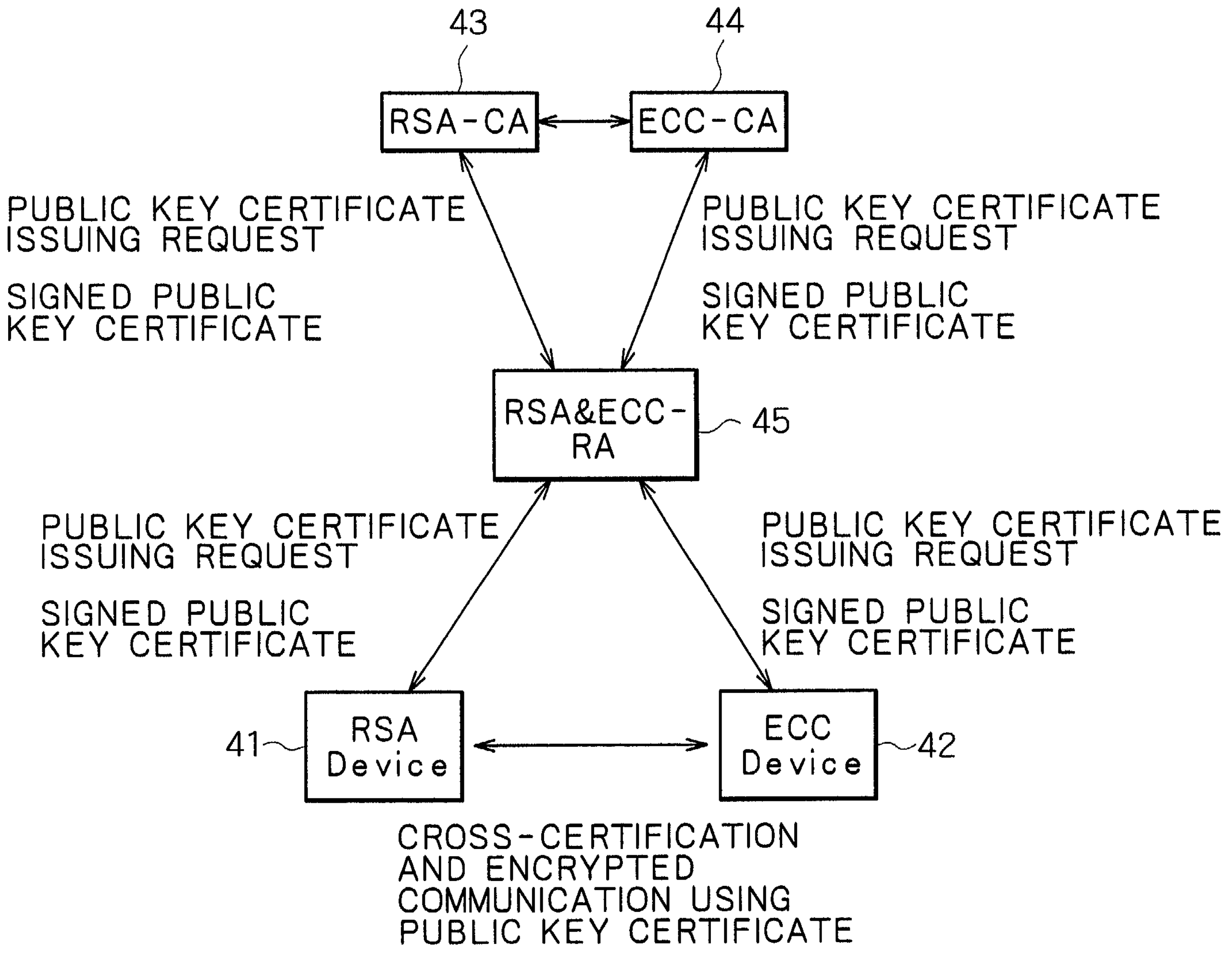

43
44
RSA-CA
ECC-CA
PUBLIC KEY CERTIFICATE ISSUING REQUEST
SIGNED PUBLIC KEY CERTIFICATE
PUBLIC KEY CERTIFICATE ISSUING REQUEST
SIGNED PUBLIC KEY CERTIFICATE
RSA&ECC-RA
45
PUBLIC KEY CERTIFICATE ISSUING REQUEST
SIGNED PUBLIC KEY CERTIFICATE
PUBLIC KEY CERTIFICATE ISSUING REQUEST
SIGNED PUBLIC KEY CERTIFICATE
41
RSA Device
ECC Device
42
CROSS-CERTIFICATION AND ENCRYPTED COMMUNICATION USING PUBLIC KEY CERTIFICATE

FIG.5

EXAMPLE OF CERTIFICATE FORMAT (BASED ON X.509 V3)

ITEMS	DESCRIPTION	SETTINGS WITH THIS IA
	Version 1	
version	VERSION OF CERTIFICATE FORMAT	V3
serial Number	CERTIFICATE SERIAL NUMBER FURNISHED BY IA	SEQUENTIAL SERIAL NUMBER
signature.algorithm Identifier algorithm parameters	CERTIFICATE SIGNATURE ALGORITHM AND PARAMETERS	·ELLIPTIC CURVE CRYPTOGRAPHY OR RSA ·PARAMETERS IN THE CASE OF ELLIPTIC CURVE CRYPTOGRAPHY ·KEY LENGTH IN THE CASE OF RSA
issuer	IA NAME (DISTINGUISHED NAME FORMAT)	NAME OF THIS IA
validity notBefore notAfter	VALIDITY OF CERTIFICATE ·STARTING DATE AND TIME ·ENDING DATE AND TIME	
subject	USER IDENTIFICATION NAME	USER DEVICE ID OR SERVICE ENTITY ID
subject Public Key Info algorithm subject Public key	USER'S PUBLIC KEY INFORMATION ·KEY ALGORITHM ·PUBLIC KEY	·ELLIPTIC CURVE CRYPTOGRAPHY OR RSA ·USER'S PUBLIC KEY
	Version 3	
authority Key Identifier key Identifier authority Cert Issuer authority Cert Serial Number	·KEY IDENTIFIER FOR SIGNATURE VERIFICATION BY IA ·KEY ID NUMBER (OCTAL) ·IA NAME (GENERAL NAME FORMAT) ·CERTIFICATE SERIAL NUMBER	
subject key Identifier	APPLICABLE WHERE MULTIPLE KEYS NEED TO BE CERTIFIED	NOT USED
key usage (0)digital Signature (1)non Repudiation (2)key Encipherment (3)data Encipherment (4)key Agreement (5)key CertSign (6)cRL Sign	THE PURPOSE OF KEY USAGE IS DESIGNATED (0)FOR DIGITAL SIGNATURE (1)FOR REPUDIATION PREVENTION (2)FOR KEY ENCRYPTION (3)FOR MESSAGE ENCRYPTION (4)FOR DISTRIBUTION OF COMMON KEY (5)FOR VERIFICATION OF SIGNATURE ON CERTIFICATE (6)FOR VERIFICATION OF SIGNATURE ON CERTIFICATE REVOCATION LIST	USAGE (0), (1), (4) AND (6) APPLY
private Key Usage Period notBefore notAfter	USAGE PERIOD OF USER'S PRIVATE KEY	USAGE PERIOD OF CERTIFICATE=USAGE PERIOD OF PUBLIC KEY=USAGE PERIOD OF PRIVATE KEY (DEFAULT)

FIG.6

policy Mappings issuer Domain Policy subject Domain Policy	NECESSARY ONLY WHEN CA IS CERTIFIED. AN ISSUER DOMAIN POLICY AND A SUBJECT DOMAIN POLICY ARE DEFINED.	NONE BY DEFAULT
supported Algorithms algorithm Identifier intended Usage intended Certificate Policies	ATTRIBUTES OF THE DIRECTORY (X.500) ARE DEFINED. WHEN THE OPPOSITE PARTY OF COMMUNICATION IS TO USE DIRECTORY INFORMATION, THAT PARTY IS INFORMED OF THE DIRECTORY ATTRIBUTES IN ADVANCE.	NONE BY DEFAULT
subject Alt Name	USER'S ALTERNATIVE NAME (GENERAL NAME FORMAT).	NOT USED
issuer Alt Name	THIS FIELD IS INCLUDED (NONE BY DEFAULT).	NONE BY DEFAULT
subject Directory Attributes	USER'S ANY ATTRIBUTES.	NOT USED
basic Constraints cA path Len Constraint	THIS FIELD SPECIFIES WHETER THE PUBLIC KEY SUBJECT TO CERTIFICATION IS TO BE SIGNED BY THE CERTIFICATE AUTHORITY (CA) OR USED BY THE USER.	USED BY USER BY DEFAULT
name Constraints permitted Subtrees base minimum maximum excluded Subtrees	USED ONLY WHEN THE SUBJECT IS CA (CA CERTIFICATION).	NONE BY DEFAULT
policy Constraints require Explicit Policy inhibit Policy Mapping	DESCRIBED HERE ARE CONSTRAINTS REQUIRING EXPLICIT POLICY IDs AND INHIBIT POLICY MAPPING FOR THE REMAINING CERTIFICATION PATHS.	
CRL Distribution Points	DESCRIBED HERE ARE POINTS AT WHICH THE USER REFERENCES THE CERTIFICATE REVOCATION LIST (CRL) TO SEE WHETHER THE CERTIFICATE IS REVOKED.	THESE POINTS SERVE AS POINTERS INDICATING WHERE THE CERTIFICATE IS REGISTERED. THE CERTIFICATE REVOCATION LIST IS MANAGED BY THE ISSUER.
SIGNATURE	ISSUER'S SIGNATURE	

FIG.7

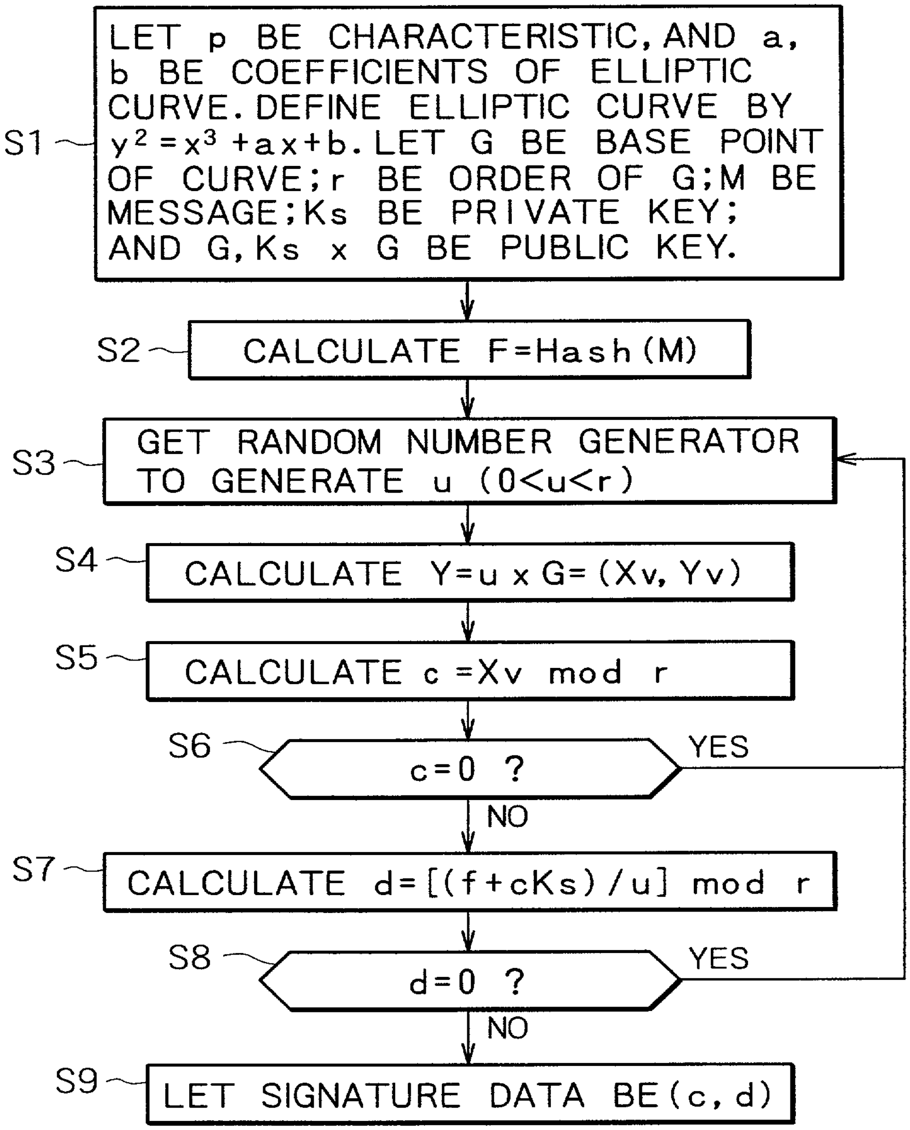

S1
LET p BE CHARACTERISTIC, AND a, b BE COEFFICIENTS OF ELLIPTIC CURVE. DEFINE ELLIPTIC CURVE BY $y^2=x^3+ax+b$. LET G BE BASE POINT OF CURVE; r BE ORDER OF G; M BE MESSAGE; Ks BE PRIVATE KEY; AND G, Ks x G BE PUBLIC KEY.
S2
CALCULATE F=Hash(M)
S3
GET RANDOM NUMBER GENERATOR TO GENERATE u (0<u<r)
S4
CALCULATE Y=u x G=(Xv, Yv)
S5
CALCULATE c =Xv mod r
S6
c=0 ?
YES
NO
S7
CALCULATE d=[(f+cKs)/u] mod r
S8
d=0 ?
YES
NO
S9
LET SIGNATURE DATA BE(c, d)

FIG.8

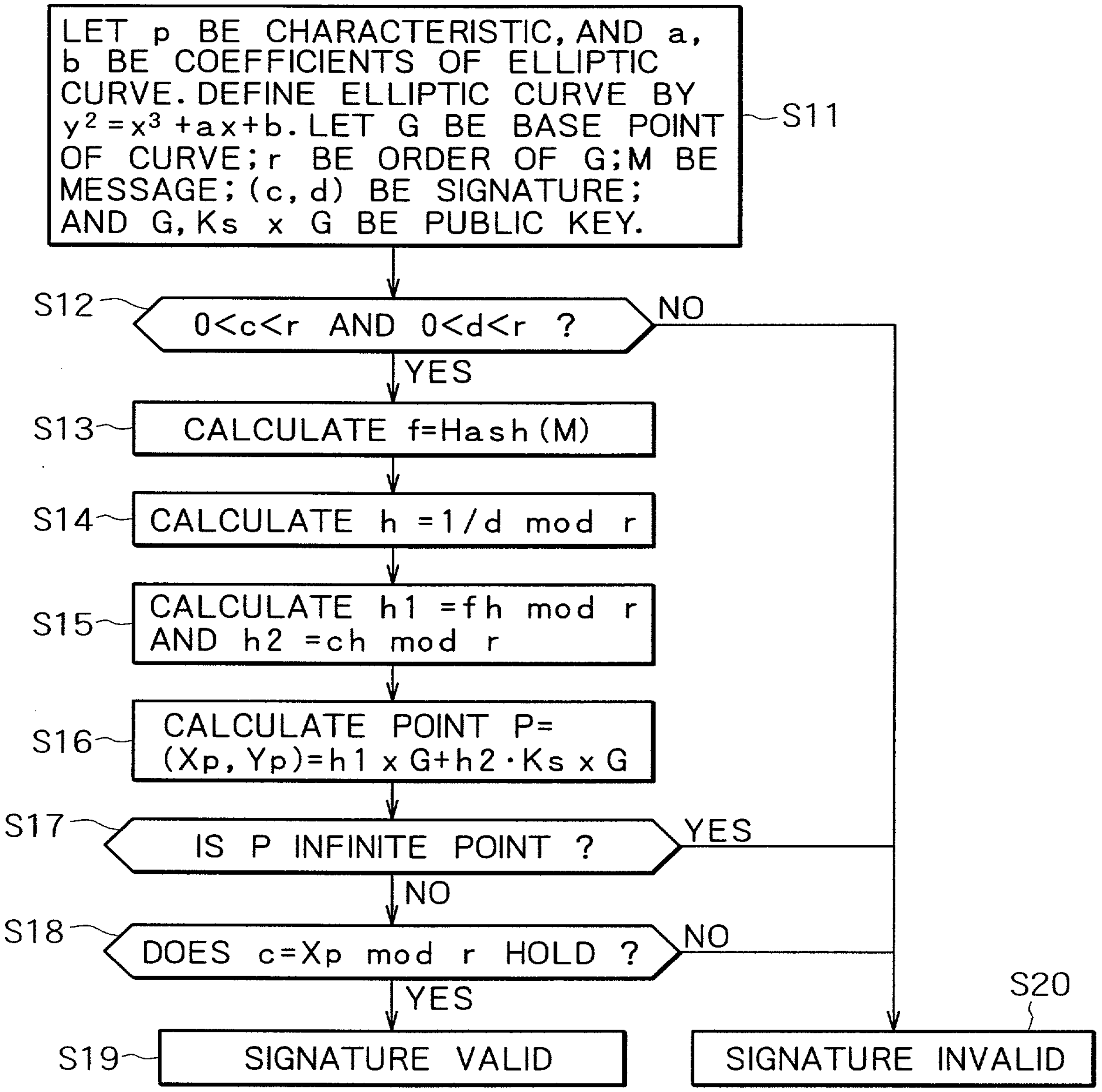

LET p BE CHARACTERISTIC, AND a, b BE COEFFICIENTS OF ELLIPTIC CURVE. DEFINE ELLIPTIC CURVE BY $y^2=x^3+ax+b$. LET G BE BASE POINT OF CURVE; r BE ORDER OF G; M BE MESSAGE; (c, d) BE SIGNATURE; AND G, Ks x G BE PUBLIC KEY.
S11
S12
0<c<r AND 0<d<r ?
NO
YES
S13
CALCULATE f=Hash (M)
S14
CALCULATE h =1/d mod r
S15
CALCULATE h1 =fh mod r AND h2 =ch mod r
S16
CALCULATE POINT P= (Xp, Yp)=h1 x G+h2・Ks x G
S17
IS P INFINITE POINT ?
YES
NO
S18
DOES c=Xp mod r HOLD ?
NO
YES
S19
SIGNATURE VALID
S20
SIGNATURE INVALID

FIG.9

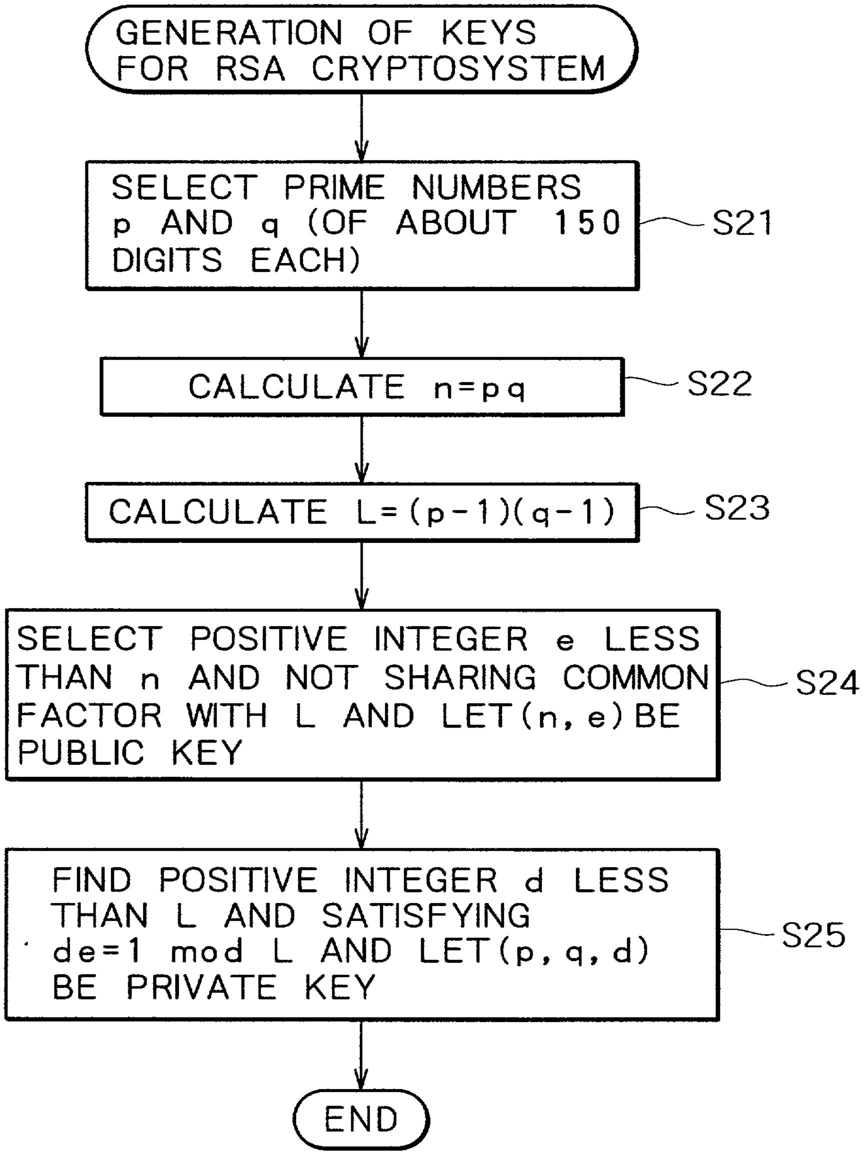

GENERATION OF KEYS FOR RSA CRYPTOSYSTEM
SELECT PRIME NUMBERS p AND q (OF ABOUT 150 DIGITS EACH)
S21
CALCULATE n=pq
S22
CALCULATE L=(p-1)(q-1)
S23
SELECT POSITIVE INTEGER e LESS THAN n AND NOT SHARING COMMON FACTOR WITH L AND LET (n, e) BE PUBLIC KEY
S24
FIND POSITIVE INTEGER d LESS THAN L AND SATISFYING de=1 mod L AND LET (p, q, d) BE PRIVATE KEY
S25
END

FIG. 10A

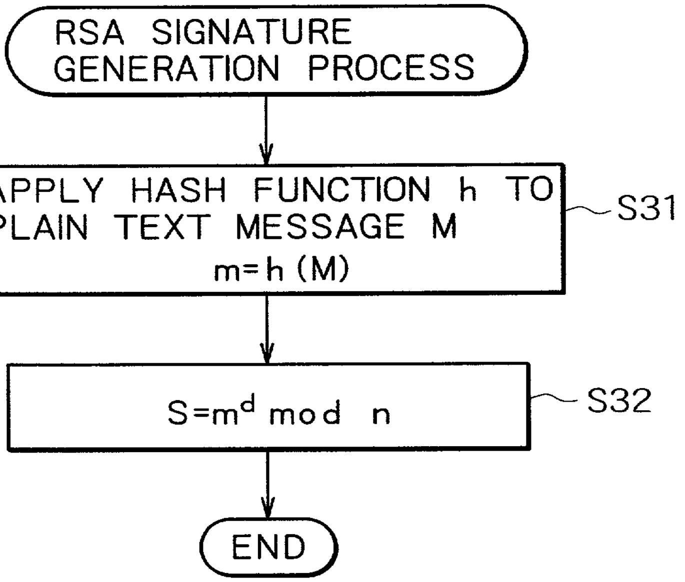


FIG. 10B

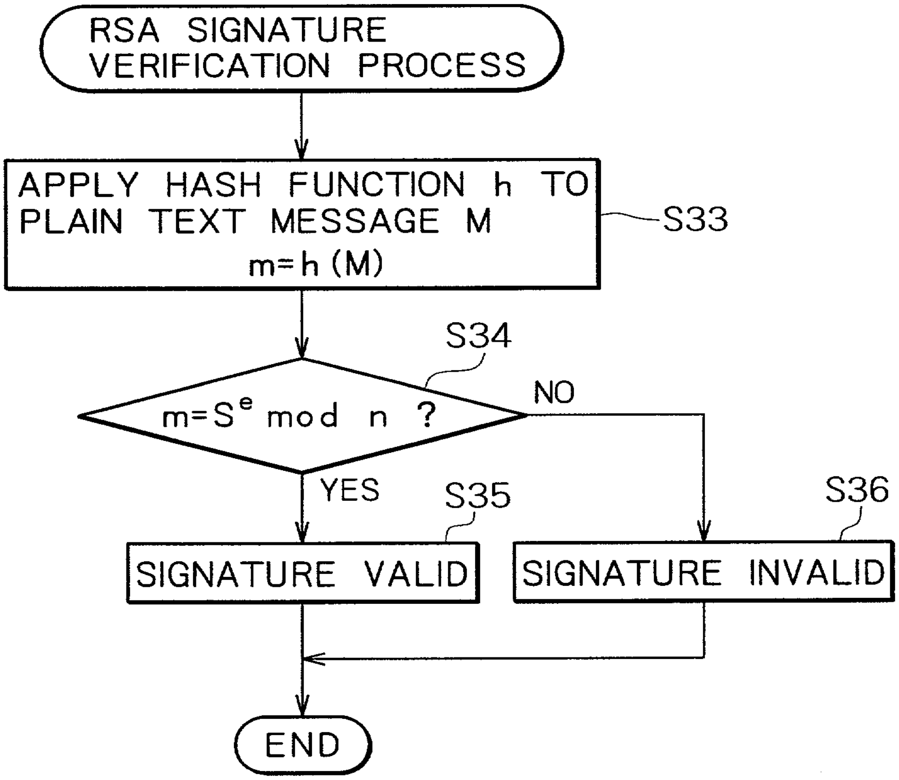


FIG. 11

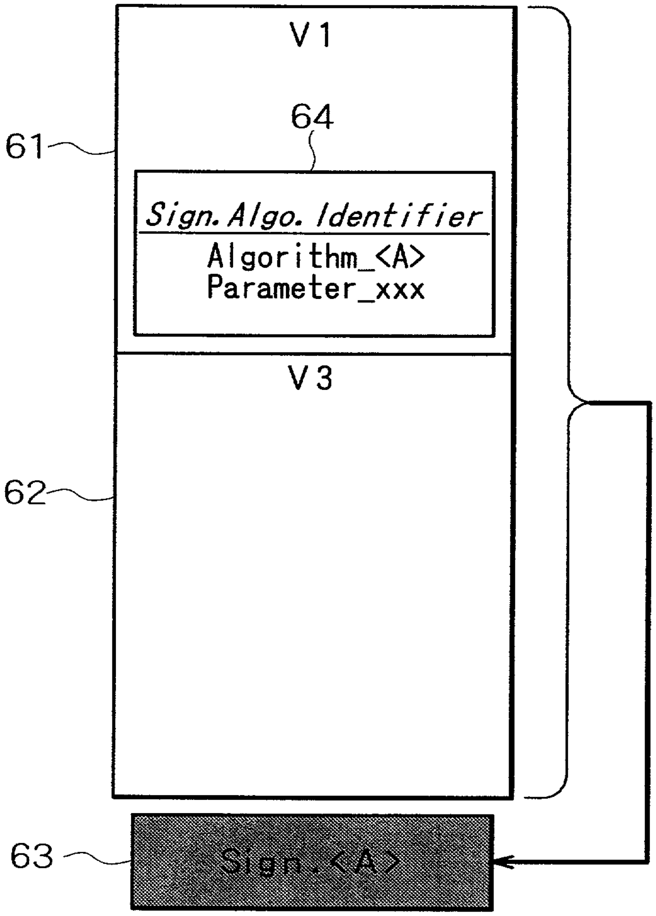

V1
64
61
Sign. Algo. Identifier
Algorithm_<A>
Parameter_xxx
V3
62
63
Sign. <A>

FIG.12

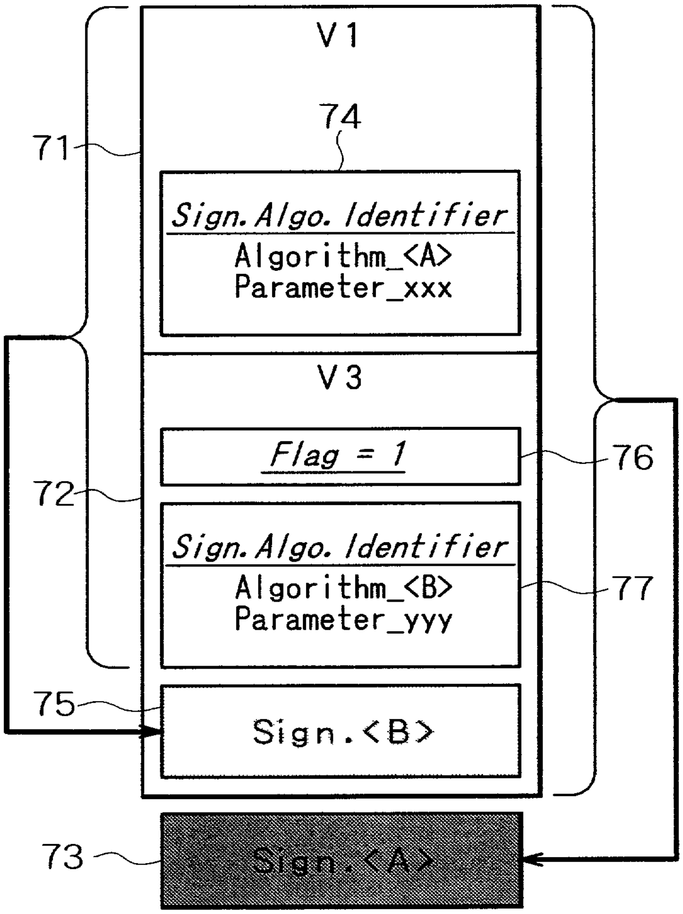

V1
74
71
Sign. Algo. Identifier
Algorithm_<A>
Parameter_xxx
V3
Flag = 1
76
72
Sign. Algo. Identifier
Algorithm_<B>
Parameter_yyy
77
75
Sign.<B>
73
Sign.<A>

FIG.13

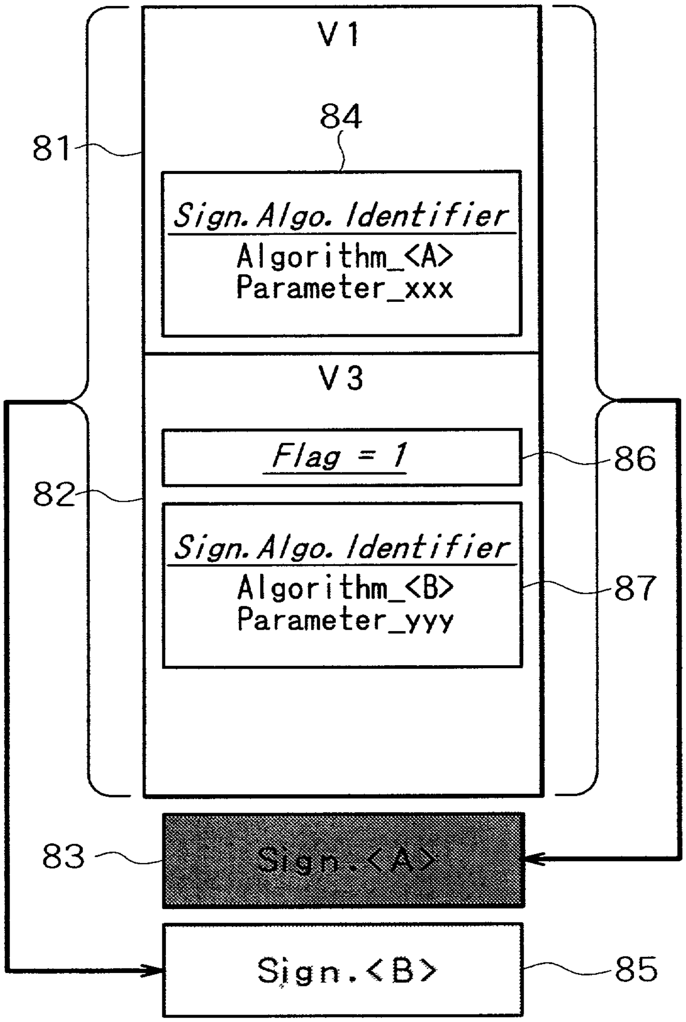

V1
84
81
Sign. Algo. Identifier
Algorithm_<A>
Parameter_xxx
V3
Flag = 1
86
82
Sign. Algo. Identifier
Algorithm_<B>
Parameter_yyy
87
83
Sign.<A>
Sign.<B>
85

FIG. 14

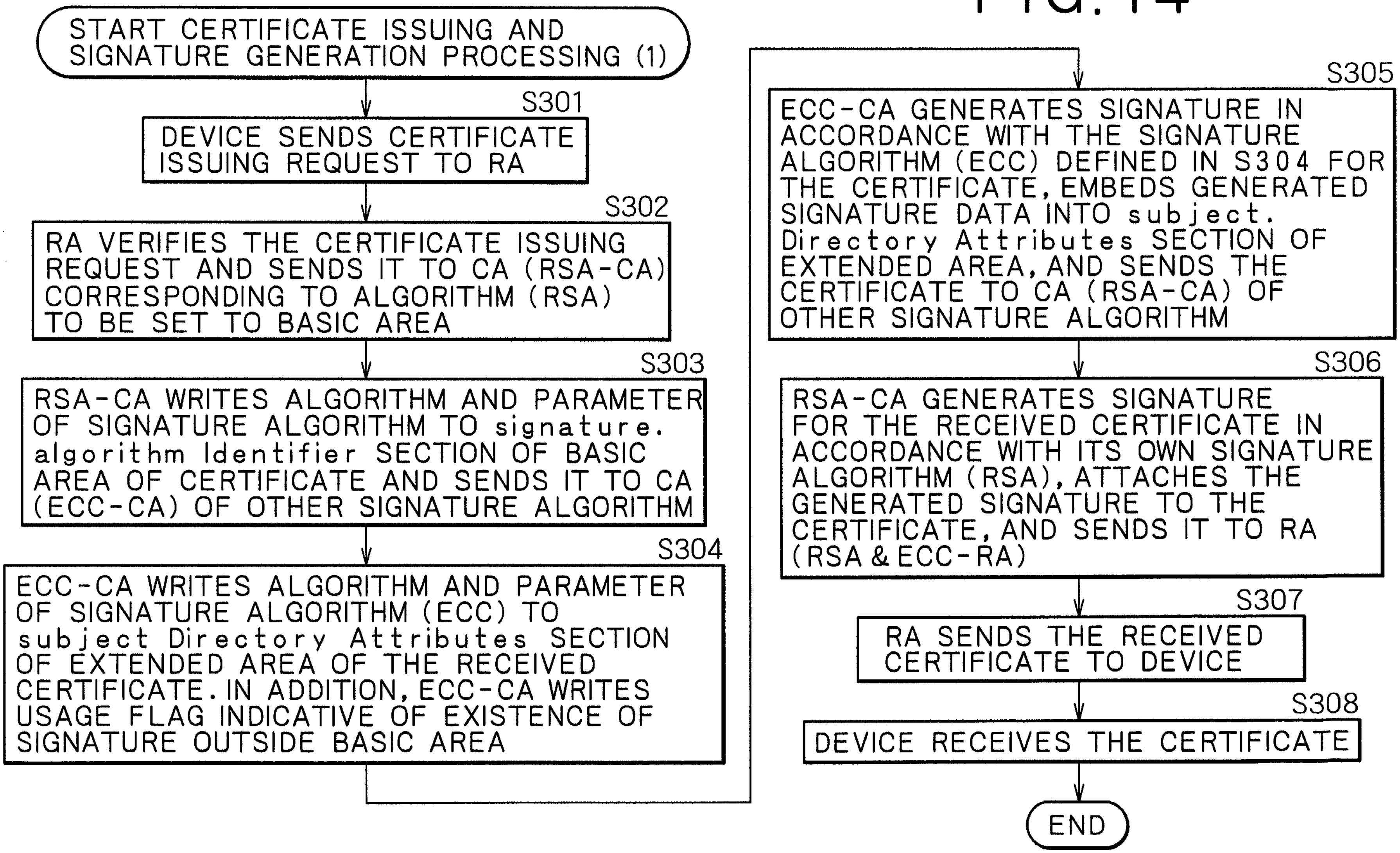

START CERTIFICATE ISSUING AND SIGNATURE GENERATION PROCESSING (1)
S301
DEVICE SENDS CERTIFICATE ISSUING REQUEST TO RA
S302
RA VERIFIES THE CERTIFICATE ISSUING REQUEST AND SENDS IT TO CA (RSA-CA) CORRESPONDING TO ALGORITHM (RSA) TO BE SET TO BASIC AREA
S303
RSA-CA WRITES ALGORITHM AND PARAMETER OF SIGNATURE ALGORITHM TO signature. algorithm Identifier SECTION OF BASIC AREA OF CERTIFICATE AND SENDS IT TO CA (ECC-CA) OF OTHER SIGNATURE ALGORITHM
S304
ECC-CA WRITES ALGORITHM AND PARAMETER OF SIGNATURE ALGORITHM (ECC) TO subject Directory Attributes SECTION OF EXTENDED AREA OF THE RECEIVED CERTIFICATE. IN ADDITION, ECC-CA WRITES USAGE FLAG INDICATIVE OF EXISTENCE OF SIGNATURE OUTSIDE BASIC AREA
S305
ECC-CA GENERATES SIGNATURE IN ACCORDANCE WITH THE SIGNATURE ALGORITHM (ECC) DEFINED IN S304 FOR THE CERTIFICATE, EMBEDS GENERATED SIGNATURE DATA INTO subject. Directory Attributes SECTION OF EXTENDED AREA, AND SENDS THE CERTIFICATE TO CA (RSA-CA) OF OTHER SIGNATURE ALGORITHM
S306
RSA-CA GENERATES SIGNATURE FOR THE RECEIVED CERTIFICATE IN ACCORDANCE WITH ITS OWN SIGNATURE ALGORITHM (RSA), ATTACHES THE GENERATED SIGNATURE TO THE CERTIFICATE, AND SENDS IT TO RA (RSA & ECC-RA)
S307
RA SENDS THE RECEIVED CERTIFICATE TO DEVICE
S308
DEVICE RECEIVES THE CERTIFICATE
END

FIG. 15

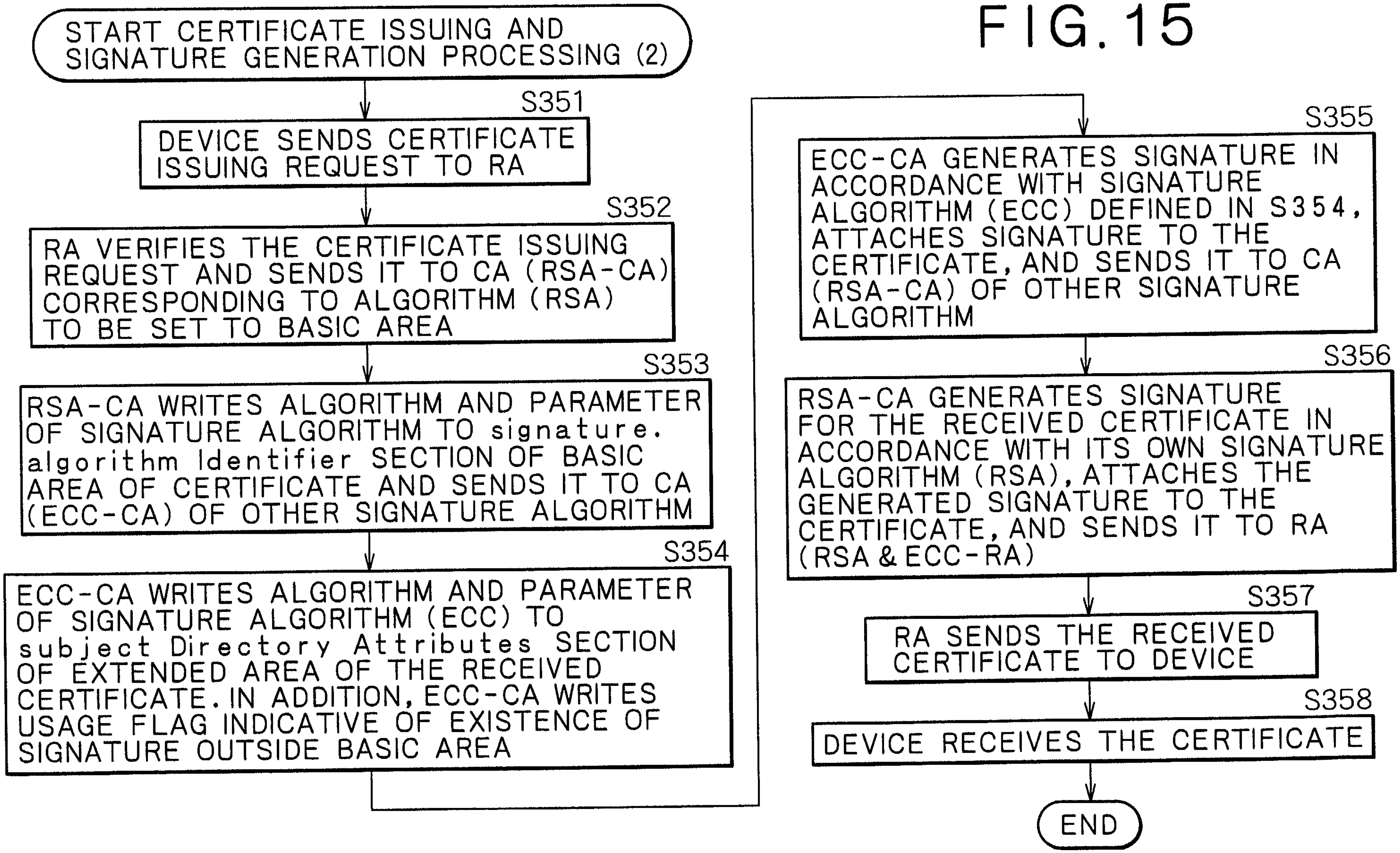

START CERTIFICATE ISSUING AND SIGNATURE GENERATION PROCESSING (2)
S351
DEVICE SENDS CERTIFICATE ISSUING REQUEST TO RA
S352
RA VERIFIES THE CERTIFICATE ISSUING REQUEST AND SENDS IT TO CA (RSA-CA) CORRESPONDING TO ALGORITHM (RSA) TO BE SET TO BASIC AREA
S353
RSA-CA WRITES ALGORITHM AND PARAMETER OF SIGNATURE ALGORITHM TO signature. algorithm Identifier SECTION OF BASIC AREA OF CERTIFICATE AND SENDS IT TO CA (ECC-CA) OF OTHER SIGNATURE ALGORITHM
S354
ECC-CA WRITES ALGORITHM AND PARAMETER OF SIGNATURE ALGORITHM (ECC) TO subject Directory Attributes SECTION OF EXTENDED AREA OF THE RECEIVED CERTIFICATE. IN ADDITION, ECC-CA WRITES USAGE FLAG INDICATIVE OF EXISTENCE OF SIGNATURE OUTSIDE BASIC AREA
S355
ECC-CA GENERATES SIGNATURE IN ACCORDANCE WITH SIGNATURE ALGORITHM (ECC) DEFINED IN S354, ATTACHES SIGNATURE TO THE CERTIFICATE, AND SENDS IT TO CA (RSA-CA) OF OTHER SIGNATURE ALGORITHM
S356
RSA-CA GENERATES SIGNATURE FOR THE RECEIVED CERTIFICATE IN ACCORDANCE WITH ITS OWN SIGNATURE ALGORITHM (RSA), ATTACHES THE GENERATED SIGNATURE TO THE CERTIFICATE, AND SENDS IT TO RA (RSA & ECC-RA)
S357
RA SENDS THE RECEIVED CERTIFICATE TO DEVICE
S358
DEVICE RECEIVES THE CERTIFICATE
END

FIG. 16

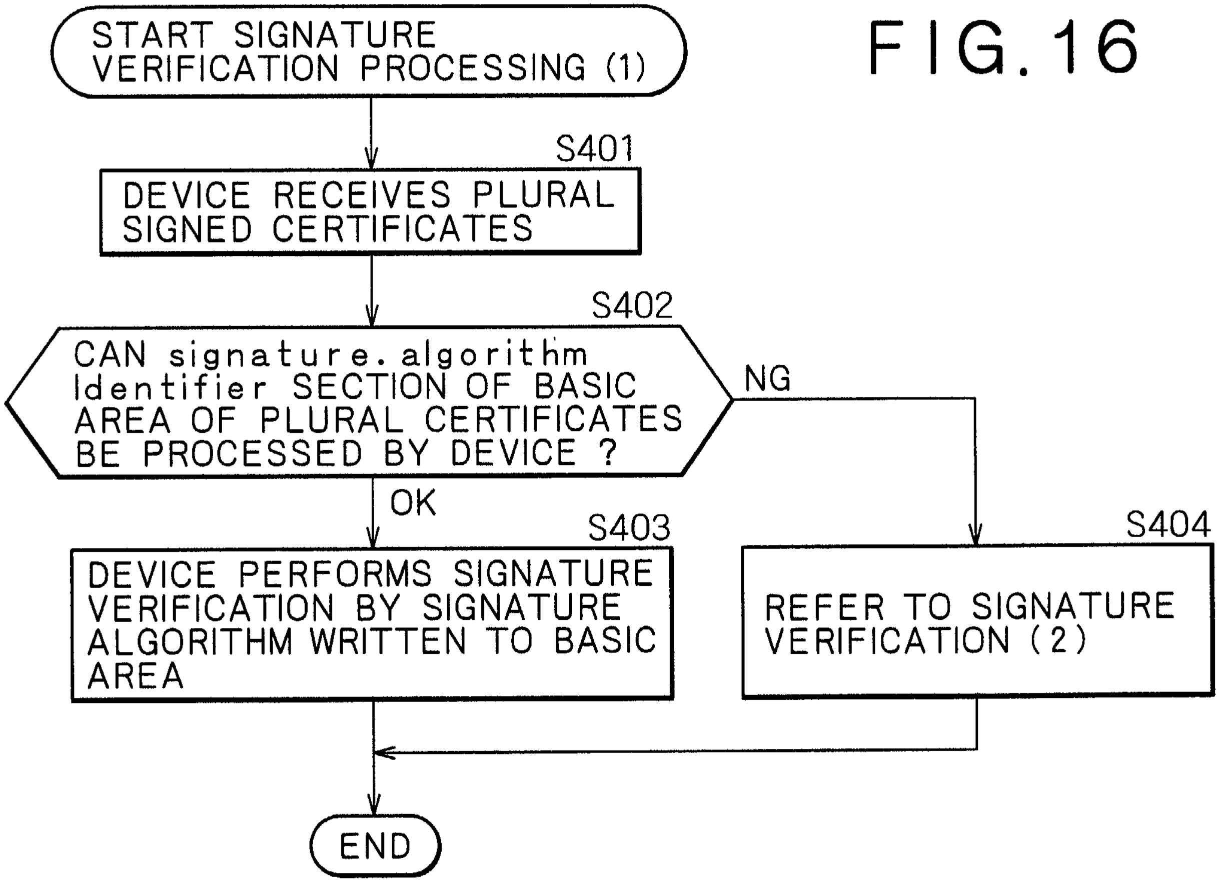
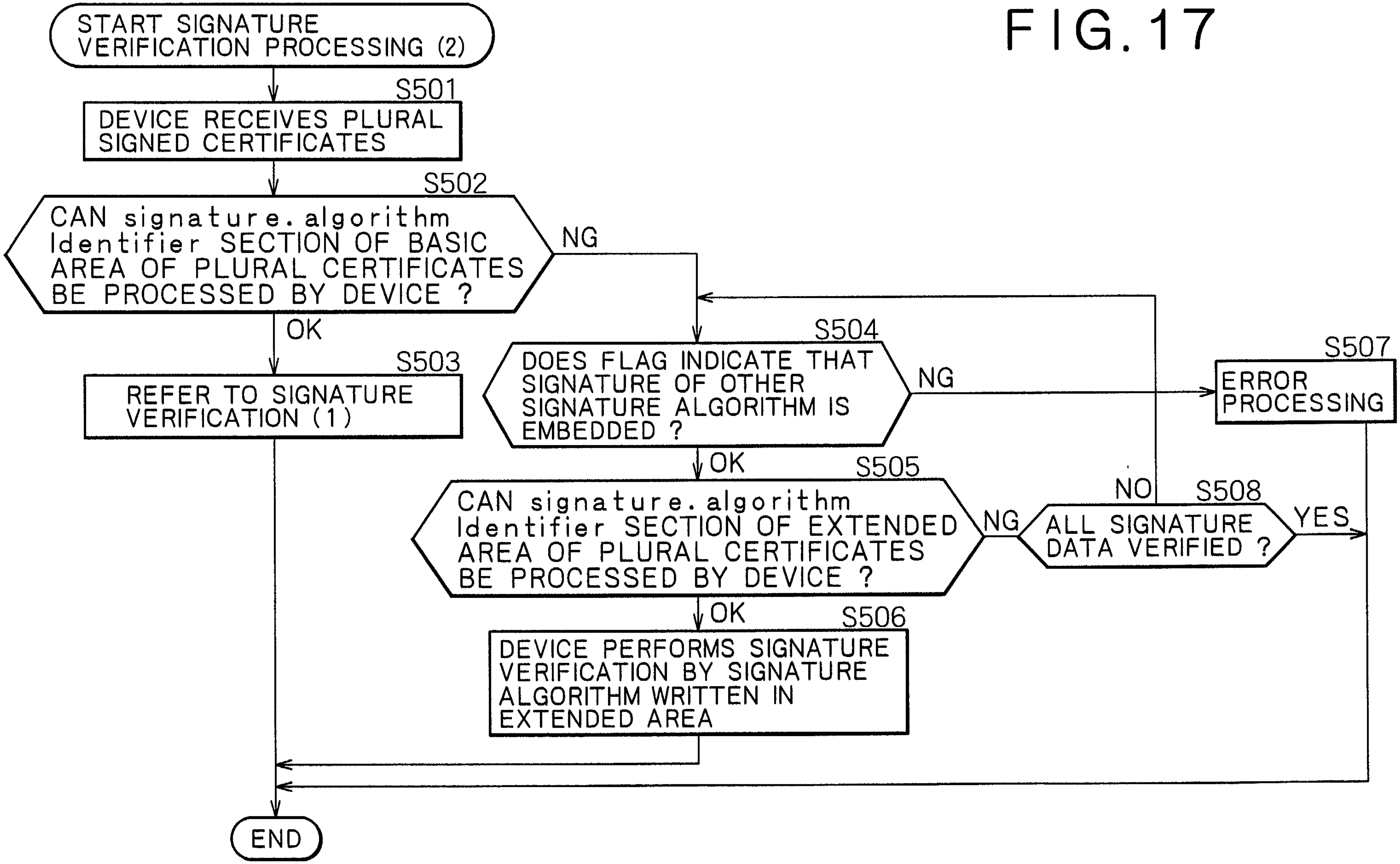

START SIGNATURE VERIFICATION PROCESSING (1)
S401
DEVICE RECEIVES PLURAL SIGNED CERTIFICATES
S402
CAN signature.algorithm Identifier SECTION OF BASIC AREA OF PLURAL CERTIFICATES BE PROCESSED BY DEVICE ?
OK
NG
S403
DEVICE PERFORMS SIGNATURE VERIFICATION BY SIGNATURE ALGORITHM WRITTEN TO BASIC AREA
S404
REFER TO SIGNATURE VERIFICATION (2)
END

FIG. 17


START SIGNATURE VERIFICATION PROCESSING (2)
S501
DEVICE RECEIVES PLURAL SIGNED CERTIFICATES
S502
CAN signature. algorithm Identifier SECTION OF BASIC AREA OF PLURAL CERTIFICATES BE PROCESSED BY DEVICE ?
OK
NG
S503
REFER TO SIGNATURE VERIFICATION (1)
S504
DOES FLAG INDICATE THAT SIGNATURE OF OTHER SIGNATURE ALGORITHM IS EMBEDDED ?
NG
OK
S507
ERROR PROCESSING
S505
CAN signature. algorithm Identifier SECTION OF EXTENDED AREA OF PLURAL CERTIFICATES BE PROCESSED BY DEVICE ?
NG
OK
S508
ALL SIGNATURE DATA VERIFIED ?
NO
YES
S506
DEVICE PERFORMS SIGNATURE VERIFICATION BY SIGNATURE ALGORITHM WRITTEN IN EXTENDED AREA
END

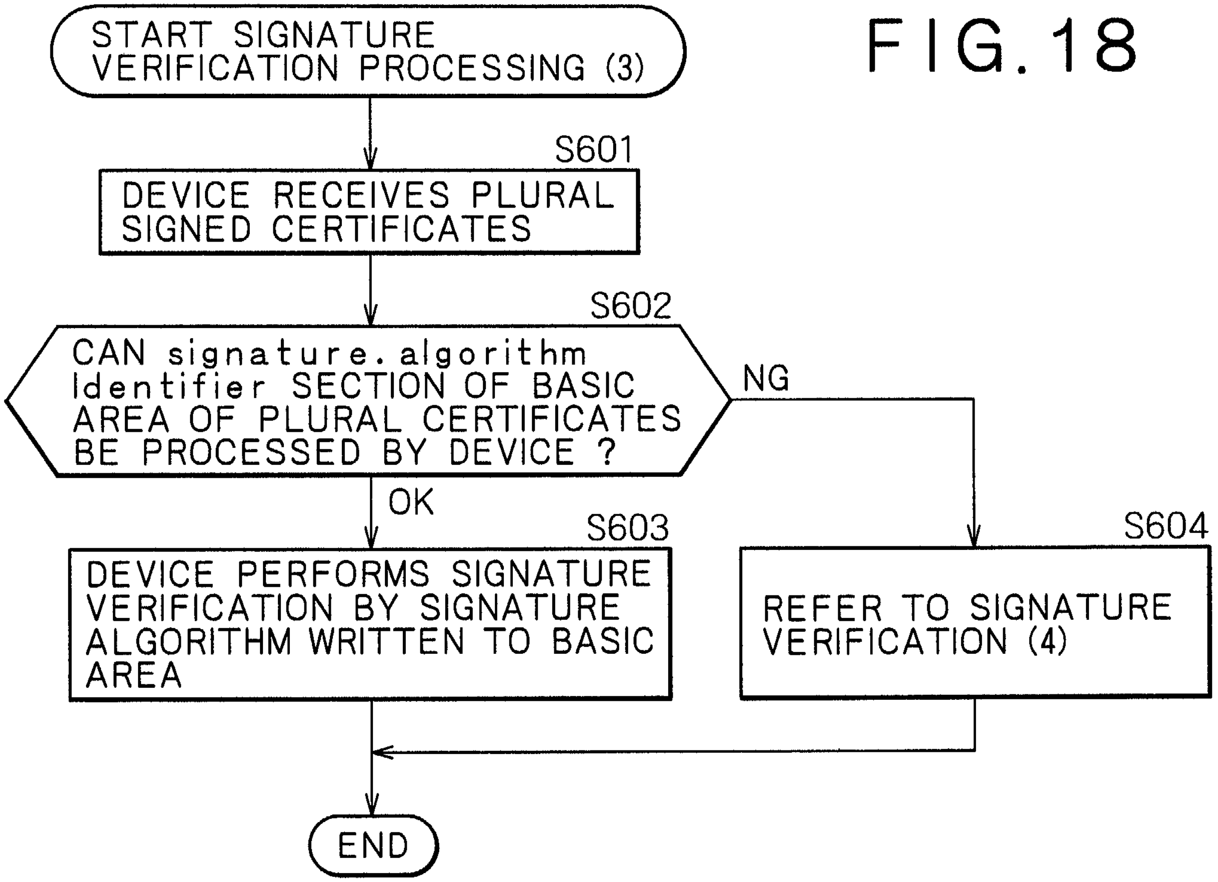

START SIGNATURE VERIFICATION PROCESSING (3)
S601
DEVICE RECEIVES PLURAL SIGNED CERTIFICATES
S602
CAN signature. algorithm Identifier SECTION OF BASIC AREA OF PLURAL CERTIFICATES BE PROCESSED BY DEVICE ?
OK
NG
S603
DEVICE PERFORMS SIGNATURE VERIFICATION BY SIGNATURE ALGORITHM WRITTEN TO BASIC AREA
S604
REFER TO SIGNATURE VERIFICATION (4)
END

FIG.18

FIG.19

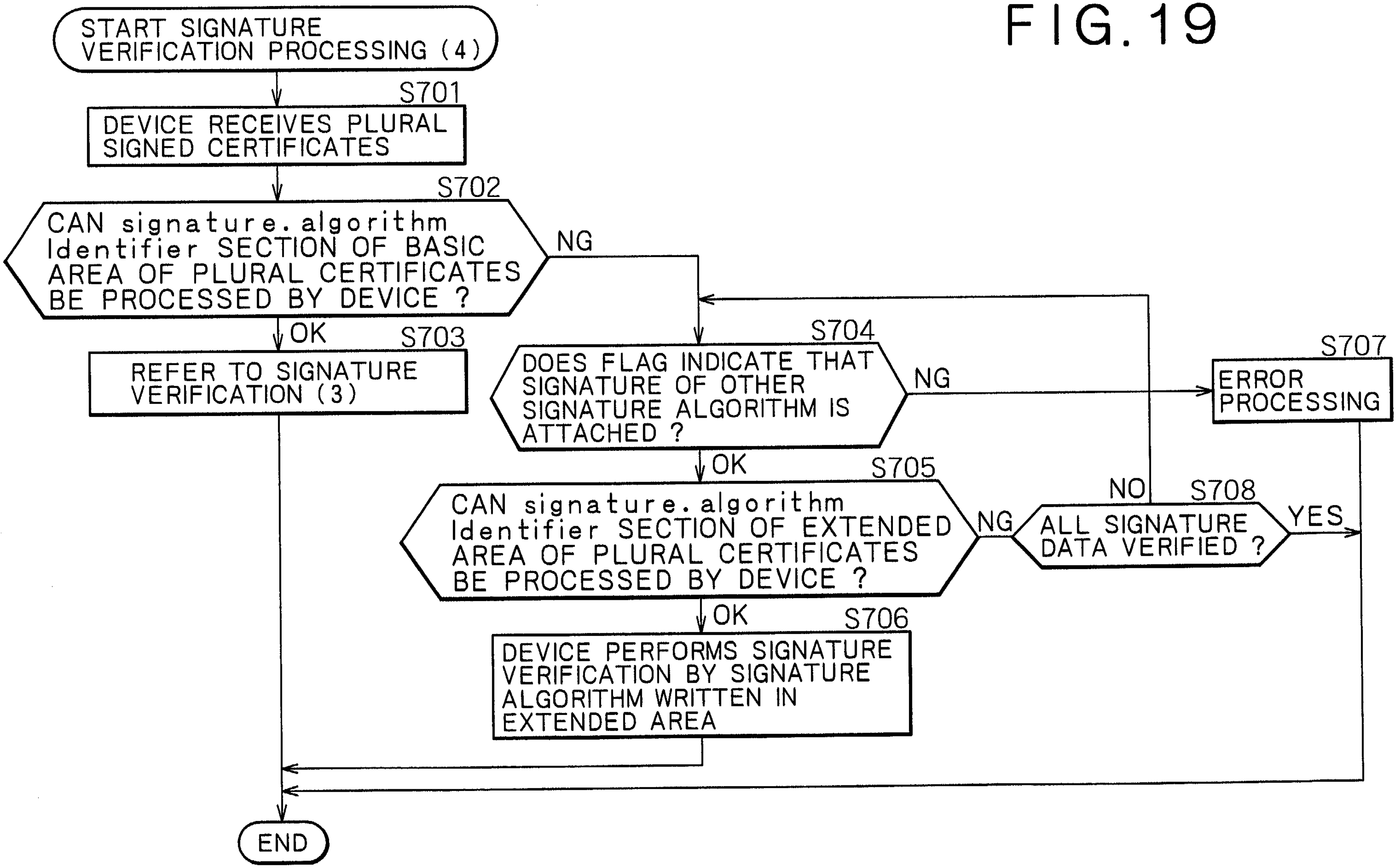

START SIGNATURE VERIFICATION PROCESSING (4)
S701
DEVICE RECEIVES PLURAL SIGNED CERTIFICATES
S702
CAN signature.algorithm Identifier SECTION OF BASIC AREA OF PLURAL CERTIFICATES BE PROCESSED BY DEVICE ?
NG
OK
S703
REFER TO SIGNATURE VERIFICATION (3)
S704
DOES FLAG INDICATE THAT SIGNATURE OF OTHER SIGNATURE ALGORITHM IS ATTACHED ?
NG
S707
ERROR PROCESSING
OK
S705
CAN signature.algorithm Identifier SECTION OF EXTENDED AREA OF PLURAL CERTIFICATES BE PROCESSED BY DEVICE ?
NG
NO
S708
ALL SIGNATURE DATA VERIFIED ?
YES
OK
S706
DEVICE PERFORMS SIGNATURE VERIFICATION BY SIGNATURE ALGORITHM WRITTEN IN EXTENDED AREA
END

FIG. 20

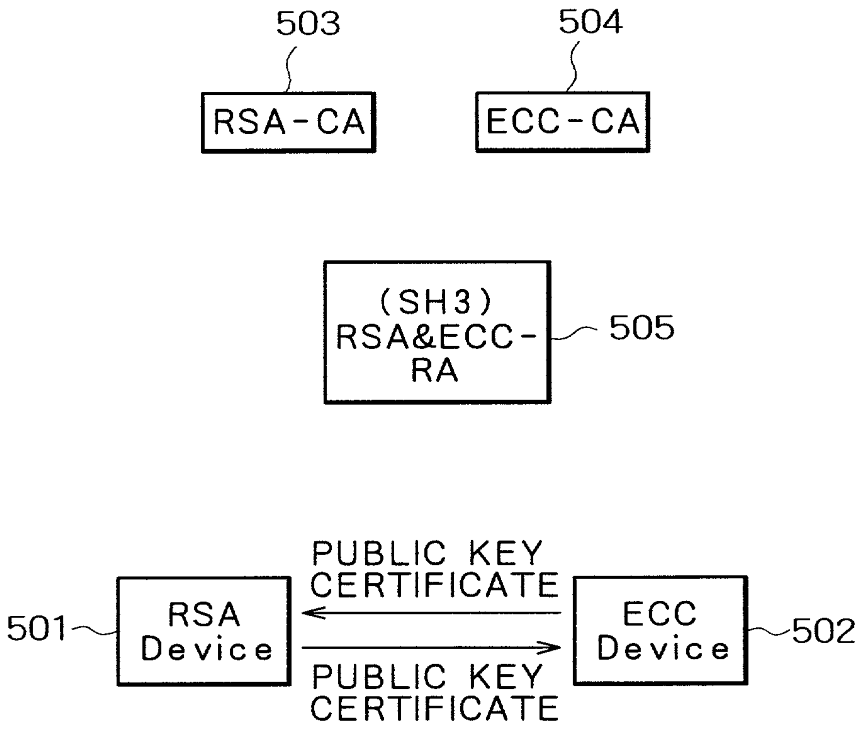

503
504
RSA-CA
ECC-CA
(SH3)
RSA&ECC-
RA
505
PUBLIC KEY
CERTIFICATE
501
RSA
Device
ECC
Device
502
PUBLIC KEY
CERTIFICATE

FIG.21

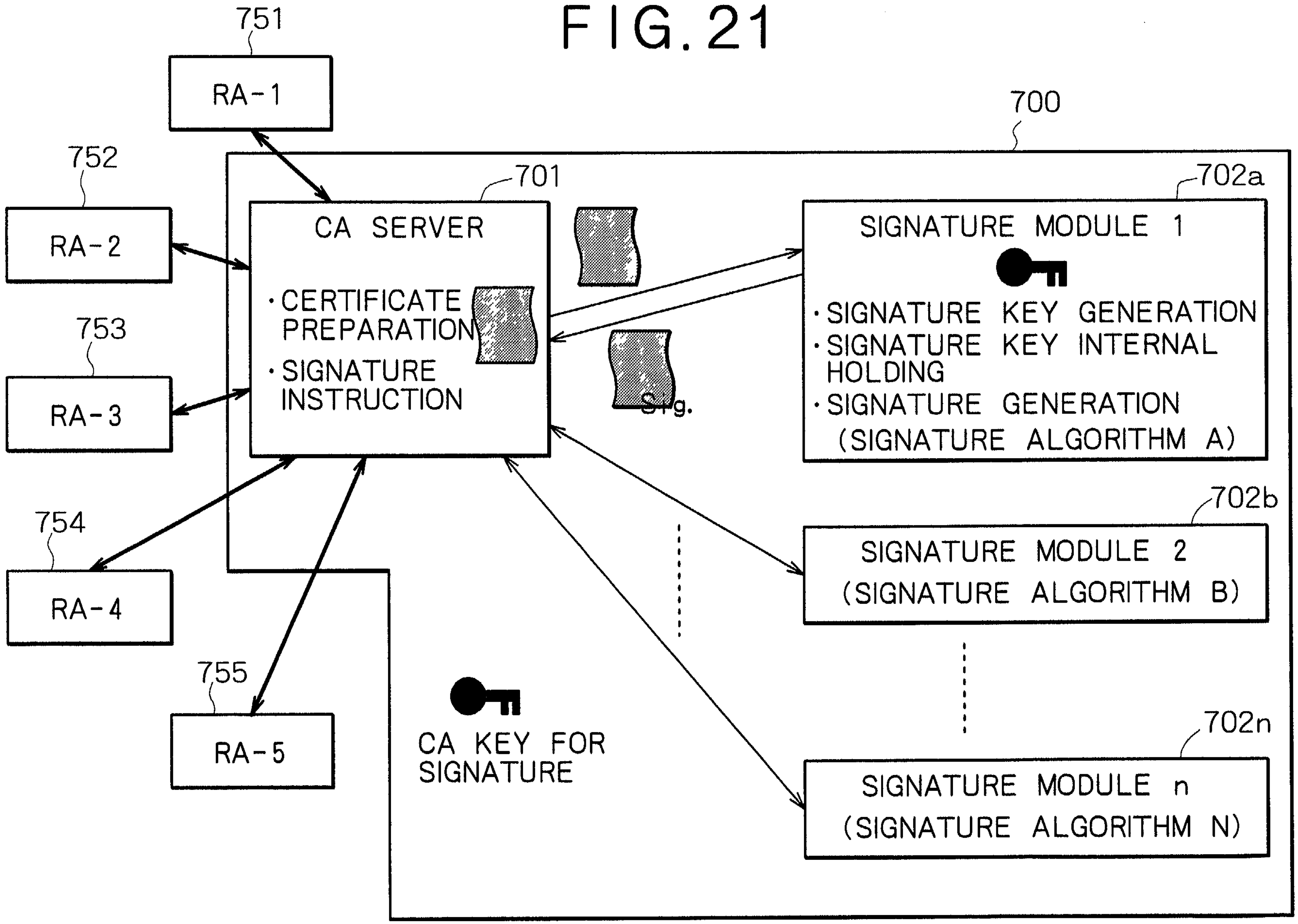

751
RA-1
752
RA-2
753
RA-3
754
RA-4
755
RA-5
700
701
CA SERVER
· CERTIFICATE PREPARATION
· SIGNATURE INSTRUCTION
Sig.
702a
SIGNATURE MODULE 1
· SIGNATURE KEY GENERATION
· SIGNATURE KEY INTERNAL HOLDING
· SIGNATURE GENERATION
(SIGNATURE ALGORITHM A)
702b
SIGNATURE MODULE 2
(SIGNATURE ALGORITHM B)
702n
SIGNATURE MODULE n
(SIGNATURE ALGORITHM N)
CA KEY FOR SIGNATURE

FIG. 22

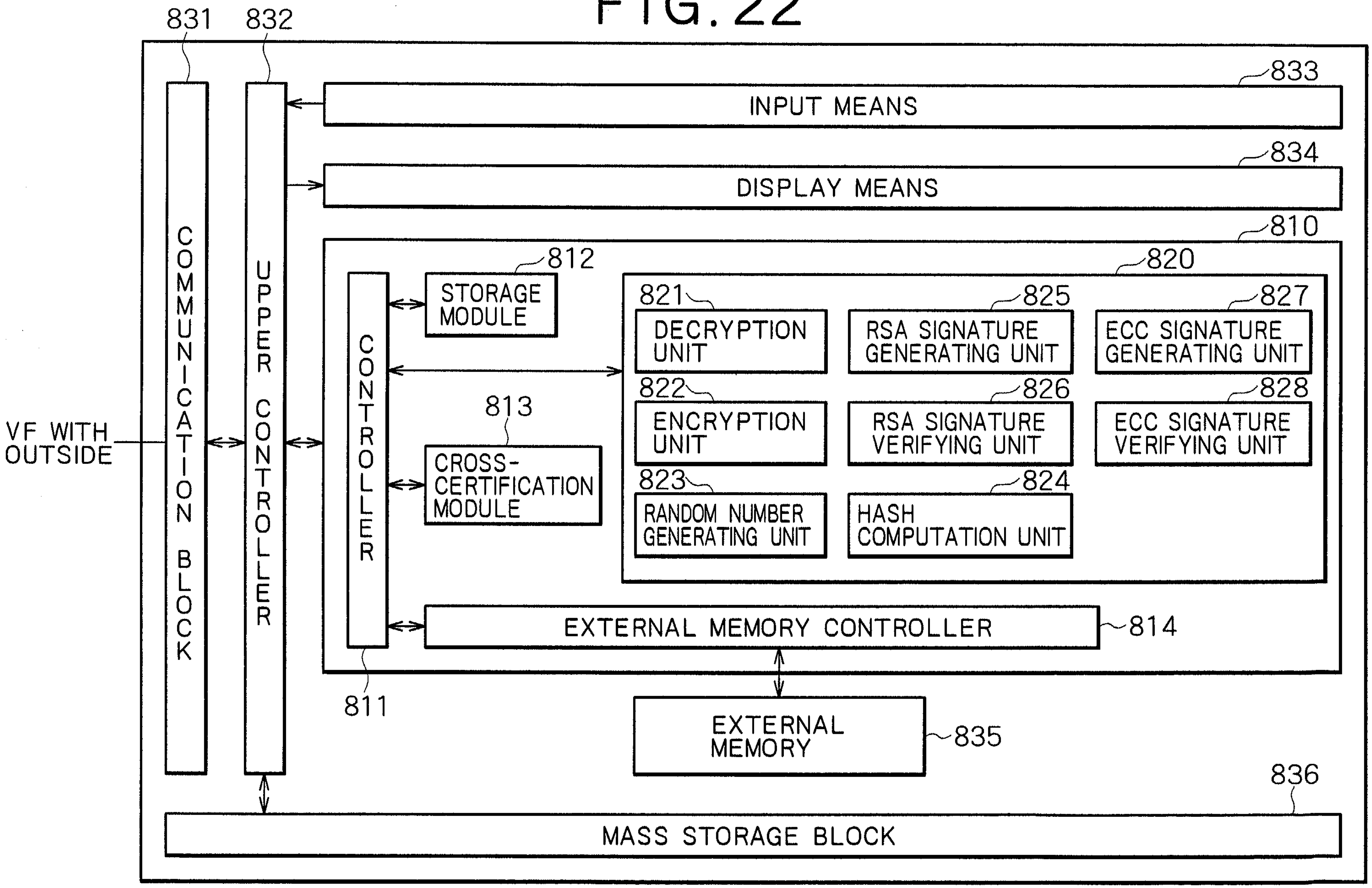
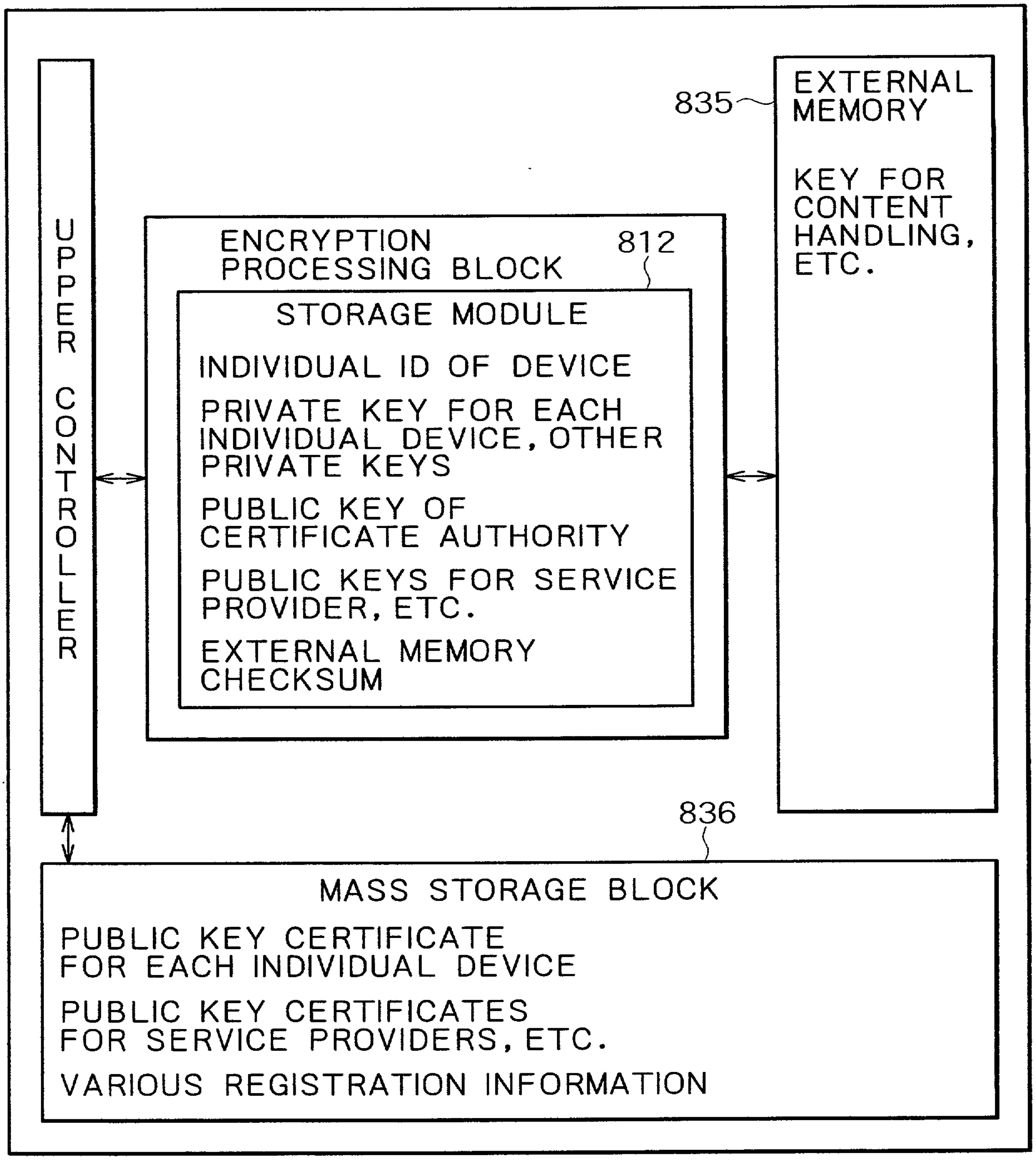

831
832
VF WITH OUTSIDE
COMMUNICATION BLOCK
UPPER CONTROLLER
INPUT MEANS
833
DISPLAY MEANS
834
810
CONTROLLER
811
STORAGE MODULE
812
CROSS-CERTIFICATION MODULE
813
820
821
DECRYPTION UNIT
822
ENCRYPTION UNIT
823
RANDOM NUMBER GENERATING UNIT
825
RSA SIGNATURE GENERATING UNIT
826
RSA SIGNATURE VERIFYING UNIT
824
HASH COMPUTATION UNIT
827
ECC SIGNATURE GENERATING UNIT
828
ECC SIGNATURE VERIFYING UNIT
EXTERNAL MEMORY CONTROLLER
814
EXTERNAL MEMORY
835
836
MASS STORAGE BLOCK

FIG. 23



UPPER CONTROLLER
ENCRYPTION PROCESSING BLOCK
812
STORAGE MODULE
INDIVIDUAL ID OF DEVICE
PRIVATE KEY FOR EACH INDIVIDUAL DEVICE, OTHER PRIVATE KEYS
PUBLIC KEY OF CERTIFICATE AUTHORITY
PUBLIC KEYS FOR SERVICE PROVIDER, ETC.
EXTERNAL MEMORY CHECKSUM
835
EXTERNAL MEMORY
KEY FOR CONTENT HANDLING, ETC.
836
MASS STORAGE BLOCK
PUBLIC KEY CERTIFICATE FOR EACH INDIVIDUAL DEVICE
PUBLIC KEY CERTIFICATES FOR SERVICE PROVIDERS, ETC.
VARIOUS REGISTRATION INFORMATION